IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	Crim. No. 1:08CR239 (GBL)
	)	
	)	Count 1: 18 U.S.C. § 371 (conspiracy)
	)	
	)	Counts 2&4: 18 U.S.C. § 1030 (computer
v.	)	intrusion)
	)	
	)	Counts 3&6: 18 U.S.C. § 2701 (unlawful
	)	access to stored communications)
	)	
ELAINE ROBERTSON CIONI,	)	Count 5: 47 U.S.C. § 223 (harassing
Defendant.	)	telephone calls)

SUPERSEDING INDICTMENT

September 2008 Term at Alexandria, Virginia

Count 1

(Conspiracy)

THE GRAND JURY CHARGES THAT:

I. Introduction

1. The Defendant ELAINE ROBERTSON CIONI had a personal relationship with BE, an individual with whom she had previously worked and who lives and works in the Eastern District of Virginia.

2. This relationship began in approximately July 2005 and continued until August 2006, when Defendant moved to Tennessee. After that date, they had intermittent contact until approximately August 2007 and were still in communication until approximately May of 2008.

3. ME is the wife of BE and is a resident of the Eastern District of Virginia.

4 AE is the daughter of BE. She attends college in the District of Columbia.

5. CE is the minor son of BE and is a resident of the Eastern District of Virginia.

6. PF is a resident of Tucson, Arizona, and is a friend of BE.

7. CR is a resident of the Eastern District of Virginia, and is an acquaintance and former co-worker of BE and the Defendant. She is also friends with a current co-worker of BE, who is named DB.

8. SW is a resident of Canada, who is an acquaintance of BE.

9. SP is a resident of Canada, who is an acquaintance of BE.

10. ST is a resident of Tennessee and is a friend of the Defendant.

II. The Conspiracy and its Objects

11. From at least October 2006 and continuing until approximately May 2008, in the Eastern District of Virginia and elsewhere, ELAINE ROBERTSON CIONI, Defendant herein, conspired and agreed to violate the federal computer intrusion statutes with others known and unknown to the government, including, but not limited to, a co-conspirator identified herein as "ST"; that is, the conspiracy had the purpose of intentionally accessing protected computers without authorization (and exceeding authorized access to protected computers) in furtherance of intentionally gaining access without authorization (and exceeding authorized access to) a facility through which an electronic communication service is provided and thereby obtaining electronic communications in electronic storage in such system, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 2701.

12. In addition to the specific illegal purpose of the conspiracy, the Defendant's motive for initiating and continuing the conspiracy was to harass, annoy, and harm BE, his family, and his acquaintances.

III. Ways, Manner, and Means of the Conspiracy

13. It was part of the conspiracy that the Defendant, in coordination with her co-conspirator ST, purchased passwords to electronic mail accounts belonging to a number of individuals associated with BE from illegal computer hacking groups on the Internet. Neither the Defendant nor ST was authorized to use these passwords to access the protected computers that hosted the electronic mail accounts stored on them.

14. It was further part of the conspiracy that the Defendant and her co-conspirator ST agreed to allow the Defendant to use ST's Paypal account to make purchases of passwords from online computer hackers for multiple electronic mail accounts associated with acquaintances, friends, co-workers, and family of BE. The Defendant also used her own Paypal account to make purchases of passwords from online hackers to further the conspiracy.

15. It was further part of the conspiracy that the Defendant and/or her co-conspirator ST obtained passwords from online computer hackers. Multiple purchases of passwords were made by participants in the conspiracy, including for a number of accounts that the government has been unable to identify. The government has, however, identified the following specific purchases of passwords:

A) BE's electronic mail account at AOL on or about October 12, 2006 and again on or about March 28, 2007;

B) ME's electronic mail account at AOL on or about November 2, 2006;

C) AE's electronic mail account at Gmail on or about November 10, 2006; and

D) PF's electronic mail account at AOL on or about November 12, 2006 and again on or about January 4, 2007.

16. It was further part of the conspiracy that the Defendant and/or her co-conspirators accessed and attempted to access Interstate electronic communications that were stored on protected computers in electronic mail accounts that were associated with at least BE, ME, AE, CE, PF, and SW from computers associated with Internet connections at the Defendant's then-place of work in Tennessee, her residence in Tennessee, and even a cruise ship on which she traveled. Copies of electronic mails associated with these accounts or fragments thereof were found on the Defendant's computers or were associated with activities that were part of the conduct involved in the conspiracy as described herein.

17. The conspiracy further sought to gather electronic mails that were associated with another acquaintance of BE, specifically SP. Evidence associated with the electronic communications of SP were recovered from the Defendant's computers and were associated with activities that were part of the conduct involved in the conspiracy.

BE AOL ACCOUNT ATTEMPTED INTRUSION

18. On or about March 10, 2008, a member of the conspiracy attempted to access, without authorization, from an Internet connection at the Defendant's then-residence in Tennessee, information contained within the AOL electronic mail account of BE. This information was stored on a protected computer operated by AOL within the Eastern District of Virginia. The attempt failed. As indicated above, a member of the conspiracy purchased the password for BE's electronic mail account at AOL from online computer hackers on or about

October 12, 2006, and again on or about March 28, 2007. BE did not authorize the Defendant or her co-conspirators to access his electronic communications.

19. In late 2006, the Defendant admitted to BE, after the fact, that she had obtained unauthorized access to his personal AOL account and had been aided in that endeavor by an unnamed individual. BE, at that time, said he forgave the Defendant. BE changed the password to his AOL electronic mail account on more than one occasion after the Defendant told him that she had accessed that account in 2006. BE was not aware of any additional attempts to gain access to his personal AOL email account and never authorized the Defendant to access his personal AOL electronic mail account.

20. At times during the conspiracy, BE was led to believe that his work electronic mail account had also been compromised, but he did not know specifically by whom or that it had actually been compromised. BE reported his suspicions to both his employer and law enforcement.

CE AOL ACCOUNT ATTEMPTED INTRUSION

21. On or about September 4, 2007, a member of the conspiracy attempted to access, without authorization, from an Internet connection at Chattanooga State Technical Community College ("CSTCC") in Tennessee, where the Defendant worked, information contained within the AOL electronic mail account of CE, the 13 year old son of BE. This information was stored on a protected computer operated by AOL within the Eastern District of Virginia. The attempt failed. Neither CE nor his parents authorized the Defendant or her co-conspirators to access his electronic communications.

ME AOL ACCOUNT INTRUSION

22. In furtherance of the conspiracy, the Defendant and/or a co-conspirator purchased the password for the AOL account belonging to ME, BE's wife, from online computer hackers on or about November 2, 2006 using ST's Paypal account. From on or about July 27, 2007 through on or about August 30, 2007, a member of the conspiracy successfully accessed ME's AOL electronic mail account in the Eastern District of Virginia multiple times, without authorization, from Internet connections at both CSTCC and the Defendant's then-residence in Tennessee. Portions of an electronic mail from sometime just before November 20, 2006 that originated from ME's AOL account were recovered from the computer assigned to the Defendant at CSTCC; this email was from ME to someone at her son's school. ME did not authorize the Defendant or her co-conspirators to access her electronic communications.

23. There were a number of unsuccessful attempted accesses of ME's AOL account during 2008. On February 26, 2008 and March 10, 2008, there were attempts to access ME's AOL account from the Defendant's then-residence. Also, on February 1, 2008, there were two failed attempts to access from an Internet connection associated with Carnival Cruises. Both the Defendant and her co-conspirator ST were on a Carnival cruise at that time. While on the cruise, ST purchased Internet access, which both ST and the Defendant used.

AE'S GMAIL ACCOUNT INTRUSION

24. In furtherance of the conspiracy, the Defendant and/or a co-conspirator purchased the password for BE's college-age daughter's Gmail account on at least one occasion (on or about November 10, 2006) using ST's Paypal account. On October 2, 2007, a member of the conspiracy successfully accessed AE's Gmail account, without authorization, from an Internet connection at

CSTCC in Tennessee, where the Defendant worked. Portions of three electronic mail messages from AE's Gmail account were recovered from the computer assigned to the Defendant at CSTCC:

A) A January 25, 2007 electronic mail message entitled "Re: address" from ME to AE;

B) A July 19, 2007 electronic mail message entitled "hi, i\'m fine. :-)" from AE to BE at his work electronic mail address; and

C) An August 1, 2007 electronic mail message entitled "rooming things" from AE to a friend of hers with an AOL account.

25. Neither AE nor her parents authorized the Defendant or her co-conspirators to access her electronic communications.

PF AOL ACCOUNT INTRUSION

26. In furtherance of the conspiracy, on at least two occasions (on or about November 12, 2006 and again on or about January 4, 2007), a member of the conspiracy purchased the password for PF's AOL account from online computer hackers. The November 2006 purchase was made using ST's Paypal account, while the January 2007 purchase was made using the Defendant's Paypal account.

27. Just three days after the purchase of PF's password for the AOL account in November 2006, BE sent an email from his work account to PF's AOL account. At some point between November 2006 and October 2007, a member of the conspiracy obtained a copy of the November 15, 2006 email from PF's AOL account. On both on or about October 22, 2007, and on or about November 15, 2007, copies of this email were mailed to BE in the Eastern District of Virginia by a member of the conspiracy. The October 22, 2007 mailing appeared to be from the

J.W. Marriott Pennsylvania Avenue Hotel in Washington, D.C., where the Defendant and her co-conspirator ST were staying at the time.

28. On or about March 10, 2008, a member of the conspiracy attempted to access, without authorization, from an Internet connection at the Defendant's then-residence in Tennessee information contained within the AOL electronic mail account of PF. This information was stored on a protected computer operated by AOL LLC within the Eastern District of Virginia. This specific attempt in 2008 failed.

29. PF did not authorize the Defendant or her co-conspirators to access her electronic communications.

SW HOTMAIL ACCOUNT INTRUSION

30. In furtherance of the conspiracy, on multiple occasions between April 28, 2008 and May 8, 2008, the Defendant and/or another member of the conspiracy, without authorization, successfully accessed the Hotmail electronic mail account of SW stored on a protected computer in California from Internet connections at the Defendant's then-residence and workplace in Tennessee.

31. Also, in furtherance of the conspiracy, on July 4, 2007, the Defendant, using her own Paypal account, made a purchase from the illegal online computer hacker group with the note "Hotmail Info." Multiple electronic mail messages that were associated with SW's Hotmail account, including one from July 8, 2007 (4 days after the hacked password purchase related to "Hotmail Info"), were found in the investigation of the conspiracy. For example, a copy of such an email dated September 26, 2007 was found on the computer assigned to the Defendant at CSTCC. Additionally, two paper copies of emails were mailed by a member of the conspiracy to

ME in the Eastern District of Virginia in September of 2007: one email was dated July 8, 2007, had the subject line "Re: Pictures," and was from BE to SW; the second email was dated August 14, 2007, had the subject line "Re: Hi," and was also from BE to SW. The envelopes for the two mailings appeared extremely similar including similar "constellation" stamps (though they had slightly different addresses for ME and one was postmarked from Baltimore, Maryland). SW did not authorize the Defendant or her co-conspirators to access her electronic communications.

32. In one of the mailings from a member of the conspiracy to BE in November 2007, a member of the conspiracy included an April 17, 2007 email from SP, an acquaintance of BE, to BE's work electronic mail address. Though there was no additional information about a specific compromise of an electronic mail account associated with SP, the computer assigned to the Defendant at CSTCC had fragments associated with SP's boat business.

CR YAHOO ACCOUNT COMPROMISED

33. In furtherance of the conspiracy, a member of the conspiracy downloaded information from the Yahoo electronic mail account associated with CR, an acquaintance and former co-worker of both BE and the Defendant. On the computer assigned to the Defendant at CSTCC, a copy of CR's Yahoo Inbox and Sent Folders from on or about May 22, 2008, were found. Also found on that computer were emails between CR and DB, a former co-worker, from on or about May 14, 2008. Also located on a computer recovered from the Defendant's residence were fragments that suggest that the computer was used to open to CR's mailbox.

34. CR, a resident of the Eastern District of Virginia, did not authorize the Defendant or her co-conspirators to access her electronic communications.

Overt Acts

35. It was further part of the conspiracy that the following acts in furtherance of and to effect the objects of the above-described conspiracy were committed in the Eastern District of Virginia, and elsewhere:

A) From on or about July 27, 2007 through on or about August 30, 2007, the Defendant and/or another member of the conspiracy successfully accessed ME's AOL account on a protected computer operated by AOL in the Eastern District of Virginia multiple times, without authorization, from Internet connections at both CSTCC and the Defendant's then-residence in Tennessee.

B) On or about September 4, 2007, the Defendant attempted to access, without authorization, from an Internet connection at CSTCC, where the Defendant worked, information contained within the AOL electronic mail account of CE, the minor son of BE. This information was stored on a protected computer operated by AOL within the Eastern District of Virginia. The attempt failed.

C) On or about October 22, 2007, a member of the conspiracy mailed through the U.S. Postal Service a copy of a November 15, 2006 email from BE's work account to PF's AOL account to BE in the Eastern District of Virginia from the J.W. Marriott Pennsylvania Avenue Hotel in Washington, D.C.

D) On or about November 15, 2007, a member of the conspiracy mailed through the U.S. Postal Service a copy of the November 15, 2006 email from BE's work account to PF's AOL account, as well as an April 17, 2007 email from SP to BE's work address, to BE in the Eastern District of Virginia.

E) On or about September 17, 2007, a member of the conspiracy mailed through the U.S. Postal Service to ME in the Eastern District of Virginia, in two envelopes, copies of two emails. The first was of an email dated July 8, 2007. The email had the subject line "Re: Pictures," and was from BE to SW. The second email was dated August 14, 2007. The email had the subject line "Re: Hi" and was from BE to SW.

F) On or about February 1, 2008, a member of the conspiracy attempted to access, without authorization, from an Internet connection associated with Carnival Cruises, information contained within the AOL electronic mail account of ME. This information was stored on a protected computer operated by AOL within the Eastern District of Virginia. The attempt failed.

G) On or about March 10, 2008, the Defendant and/or another member of the conspiracy attempted to access, without authorization, from an Internet connection at the Defendant's then-residence in Tennessee information contained within the AOL electronic mail account of PF. This information was stored on a protected computer operated by AOL within the Eastern District of Virginia. This attempt in 2008 failed. Similar attempts were made on that same date from the Defendant's residence in Tennessee on the AOL electronic mail accounts of BE and ME stored in the Eastern District of Virginia.

(All in violation of Title 18, United States Code, Section 371).

COUNT TWO

(Unauthorized Access to a Protected Computer)

1. All previous allegations of this Superseding Indictment are incorporated herein by reference.

2. On various dates beginning on or about November 20, 2006 and continuing until at least on or about March 10, 2008, in the Eastern District of Virginia and elsewhere, the defendant, ELAINE ROBERTSON CIONI, did intentionally access and attempt to access a computer without authorization and exceed and attempt to exceed authorized access to a computer and thereby did obtain and attempt to obtain information from a protected computer used in interstate and foreign commerce, and such conduct involved an interstate communication, in furtherance of criminal and tortious acts committed in violation of the laws of the United States; that is, CIONI accessed and attempted to access, without authorization, a protected computer operated by AOL within the Eastern District of Virginia and obtained and attempted to obtain information (i.e., ME's unopened electronic communications) stored on that protected computer, by means of electronic communications from Tennessee and elsewhere, in furtherance of a violation of Title 18, United States Code, Section 2701.

(All in violation of Title 18 United States Code, Sections 2, 1030(a)(2)(C) and (c)(2)(B)(i)).

COUNT THREE

(Unlawful Access to Stored Electronic Communications)

1. All previous allegations of this Superseding Indictment are incorporated herein by reference.

2. On various dates beginning on or around November 12, 2007 and continuing until at least on or around March 10, 2008, within the Eastern District of Virginia, and elsewhere, the defendant, ELAINE ROBERTSON CIONI, intentionally and without authorization, accessed and attempted to access a facility through which an electronic communication service is provided, as defined in Title 18, United States Code, Section 2510(15), and did intentionally exceed or attempt to exceed authorized access to that facility, and thereby obtain an electronic communication while the communication was in electronic storage in such system, in furtherance of criminal and tortious acts committed in violation of the laws of the United States; that is, CIONI gained and attempted to gain unauthorized access to the AOL account of PF, located on a computer operated by AOL within the Eastern District of Virginia, and obtained and attempted to obtain unopened electronic mail messages in PF's account by means of electronic communications from Tennessee and elsewhere, in furtherance of a violation of Title 18, United States Code, Section 371.

(All in violation of Title 18, United States Code, Sections 2 and 2701(a)(1), (a)(2) and (b)(1)(A)).

COUNT FOUR

(Unauthorized Access to a Protected Computer)

1. All previous allegations of this Superseding Indictment are incorporated herein by reference.

2. On or about March 10, 2008, in the Eastern District of Virginia and elsewhere, the Defendant, ELAINE ROBERTSON CIONI, did intentionally attempt to access a computer without authorization and exceed authorized access to a computer and thereby did seek to obtain information from a protected computer used in interstate and foreign commerce, and such conduct involved an interstate communication, in furtherance of criminal acts committed in violation of the laws of the United States; that is, CIONI intentionally attempted to access, without authorization, a protected computer operated by AOL within the Eastern District of Virginia and obtain information contained in PF's electronic mail account by means of interstate electronic communications from Tennessee and elsewhere, in furtherance of violations of Title 18, United States Code, Section 2701.

(All in violation of Title 18, United States Code, Sections 2, 1030(a)(2)(C) and (c)(2)(B)(i)).

COUNT FIVE

(Harassing Telephone Calls)

1. All previous allegations of this Superseding Indictment are incorporated herein by reference.

2. On various dates beginning on or about March 29, 2007 and continuing to on or about May 30, 2008, within the Eastern District of Virginia, and elsewhere, the Defendant, ELAINE ROBERTSON CIONI, knowingly made interstate telephone calls or utilized an interstate telecommunications device (often without disclosing her identity) and with the intent to annoy, abuse, threaten, and harass a person at the called number or who received the communication; that is, CIONI made calls from Tennessee and elsewhere to the Eastern District of Virginia and elsewhere, often using technology to hide her identity by making the telephone calls appear to originate from telephone numbers other than her own and by failing to identify herself when asked by the person at the called number. During the course of her conduct, CIONI made more than 300 harassing calls to BE, his family, or his co-workers.

(All in violation of Title 47, United States Code, Section 223(a)(1)(C)).

COUNT 6

(Unlawful Access to Stored Wire Communications)

1. All previous allegations of this Superseding Indictment are incorporated herein by reference.

2. On various dates beginning on or about February 26, 2007 and continuing until on or about April 25, 2007, within the Eastern District of Virginia, and elsewhere, the Defendant, ELAINE ROBERTSON CIONI, did intentionally and, without authorization, access a facility through which an electronic communication service is provided, as defined in Title 18, United States Code, Section 2510(15), and thereby obtained wire communications while the communications were in electronic storage in such system, in furtherance of a criminal or tortious act in violation of the laws of the United States; that is, CIONI gained unauthorized access to the T-Mobile voicemail account assigned to BE by his employer and obtained unopened voicemail messages in BE's account, in furtherance of violations of Title 47, United States Code, Section 223.

(All in violation of Title 18, United States Code, Section 2701(a)(1), (a)(2) and (b)(1)(A)).

A TRUE BILL

Pursuant to the E-Government Act,
the original of this page has been filed
under seal in the Clerk's Office.

FOREPERSON OF THE GRAND JURY

DATE: September 11, 2008

CHUCK ROSENBERG
United States Attorney

Jay V. Prabhu
Assistant United States Attorney

Michelle Kane
Trial Attorney
U.S. Department of Justice
Computer Crime & Intellectual Property Section